UC1: Tạo chỉ định

Use Case ID	UC-QLCD-01
Use Case Name	Tạo chỉ định
Actor	Bác sĩ trong phòng khám, Bác sĩ ngoài phòng khám
Description	Cho phép bác sĩ tạo mới một chỉ định xét nghiệm cho bệnh nhân, bao gồm nhập thông tin liên quan và lưu chỉ định vào hệ thống.
Priority	Must have
Trigger	Bác sĩ chọn chức năng “Tạo chỉ định” trong hệ thống hoặc gọi API từ bên ngoài
Pre-Condition	- Bác sĩ đã đăng nhập hệ thống hoặc đã xác thực API - Bệnh nhân đã có hồ sơ/mã định danh trong hệ thống
Post-Condition	- Chỉ định mới được lưu thành công vào hệ thống và được gửi cho bệnh nhân - Các xét nghiệm được gợi ý (nếu có) được ghi nhận
Basic Path/ Flow	1. Bác sĩ chọn chức năng “Tạo chỉ định” trong hệ thống hoặc gọi API từ bên ngoài 2. Hệ thống hiển thị form nhập liệu 3. Bác sĩ nhập thông tin: bệnh nhân, loại xét nghiệm, lý do, ghi chú 4. Hệ thống gợi ý các xét nghiệm liên quan (nếu có) 5. Bác sĩ xác nhận 6. Hệ thống hiển thị thông báo thành công
Alternative Path/ Flow	3a. Chọn mẫu chỉ định có sẵn 3a1. Bác sĩ chọn từ danh sách “mẫu chỉ định” theo bệnh lý hoặc gói xét nghiệm. 3a2. Hệ thống tự động điền thông tin loại xét nghiệm tương ứng vào form. 3a3. Bác sĩ chỉnh sửa lại trước khi xác nhận (nếu cần) 3a4. Tiếp tục bước 5,6 của basic flow
Exception Path/ Flow	3e. Mất kết nối mạng khi đang nhập thông tin

	3e1. Trong lúc bác sĩ đang nhập dữ liệu vào form tạo chỉ định, kết nối bị gián đoạn. 3e2. Hệ thống không thể gửi dữ liệu hoặc lưu nháp. 3e3. Hiển thị thông báo "Kết nối mạng bị gián đoạn. Vui lòng kiểm tra lại." 3e4. Use case kết thúc 5e. Mất phiên đăng nhập (session timeout) 5e1. Trước khi bác sĩ nhấn "Xác nhận", hệ thống kiểm tra và phát hiện phiên làm việc đã hết hạn. 5e2. Hệ thống chuyển về màn hình đăng nhập, không thể lưu chỉ định. 5e3. Use case kết thúc 6e. Lỗi hệ thống khi lưu chỉ định 6e1. Sau khi bác sĩ nhấn "Xác nhận", hệ thống gặp lỗi server/database trong quá trình lưu. 6e2. Hiển thị thông báo: "Không thể tạo chỉ định. Vui lòng thử lại sau." 6e3. Use case kết thúc 6f. Token API hết hạn (đối với bác sĩ ngoài phòng khám) 6f1. Bác sĩ ngoài gửi request tạo chỉ định qua API nhưng token không hợp lệ hoặc đã hết hạn. 6f2. Hệ thống phản hồi lỗi 401 Unauthorized.
Business Rule	BR-01: Chỉ bác sĩ có quyền "Tạo chỉ định" mới được thực hiện chức năng này. BR-02: Chỉ định phải được liên kết với một mã bệnh nhân hợp lệ đã có trong hệ thống. BR-03: Mỗi chỉ định bắt buộc phải có tối thiểu 01 loại xét nghiệm và lý do chỉ định. BR-04: Mỗi chỉ định phải chứa đầy đủ thông tin: tên bác sĩ, thời gian chỉ định, danh sách xét nghiệm, ghi chú (nếu có). BR-05: Hệ thống không cho phép tạo chỉ định mới nếu có chỉ định tương tự chưa hoàn tất trong vòng X ngày (cấu hình theo từng loại xét nghiệm). BR-06: Các xét nghiệm được gợi ý dựa trên: lý do khám, chẩn đoán ban đầu hoặc tiền sử bệnh của bệnh nhân (nếu có).

	BR-07: Sau khi tạo thành công, chỉ định được chuyển trạng thái "Chờ tiếp nhận mẫu" và gửi thông báo cho bộ phận xét nghiệm. BR-08: Mọi chỉ định phải được lưu kèm dấu thời gian và ID bác sĩ phụ trách, phục vụ cho tra cứu và đối chiếu sau này. BR-09: Một bác sĩ chỉ được tạo chỉ định trong ca làm việc được phân công (nếu áp dụng lịch làm việc). BR-10: Nếu bác sĩ tạo chỉ định từ API phòng khám đối tác, chỉ định phải được xác thực qua token và mapping ID bệnh nhân.
Non-Functional Requirement	NFR‑01 – Thời gian phản hồi: Hệ thống phải xử lý và phản hồi việc tạo chỉ định ≤ 2 giây (95 percentile). NFR‑02 – Tính sẵn sàng: Chức năng tạo chỉ định phải đạt uptime ≥ 99.9%/tháng, vì đây là nghiệp vụ cốt lõi. NFR‑03 – Bảo mật & phân quyền: Chỉ người dùng đã đăng nhập và có vai trò bác sĩ (hoặc được ủy quyền) mới được truy cập tính năng này. NFR‑04 – Xử lý đồng thời: Hệ thống phải đảm bảo tạo được ≥ 200 chỉ định/phút trong môi trường sản xuất mà không lỗi ghi dữ liệu. NFR‑05 – Tính toàn vẹn dữ liệu: Việc tạo chỉ định phải là giao dịch toàn vẹn (ACID): nếu bất kỳ bước nào thất bại (ví dụ: lưu xét nghiệm), toàn bộ thao tác bị rollback. NFR‑06 – Tương thích thiết bị: Form tạo chỉ định phải hoạt động chính xác trên thiết bị máy tính bàn, máy tính bảng, và thiết bị đầu cuối chuyên dụng tại phòng khám. NFR‑07 – Khả năng mở rộng: Hệ thống cần đáp ứng khả năng xử lý tối thiểu 1 triệu chỉ định/năm mà không ảnh hưởng hiệu năng truy xuất và báo cáo.

UC 2: Thông báo khi có kết quả xét nghiệm

Use Case ID	UC-LS-002
Use Case Name	Thông báo khi có kết quả xét nghiệm
Actor	Hệ thống Lab (HT Lab), Hệ thống, Bác sĩ, Bệnh nhân, BS PK ngoài
Description	Khi hệ thống Lab trả kết quả xét nghiệm, hệ thống sẽ gửi thông báo cho các bên liên quan để họ biết rằng kết quả đã sẵn sàng để xem.

Priority	Must have
Trigger	Hệ thống Lab trả kết quả xét nghiệm thành công về hệ thống quản lý.
Pre-Condition	Kết quả xét nghiệm đã được xác nhận và đẩy từ hệ thống Lab vào hệ thống chính.
Post-Condition	Các bên liên quan (bác sĩ, bệnh nhân, phòng khám ngoài) nhận được thông báo về kết quả xét nghiệm.
Basic Path/ Flow	1. Hệ thống Lab trả kết quả xét nghiệm thành công về hệ thống quản lý 2. HT Lab trả kết quả xét nghiệm về hệ thống. 3. Hệ thống ghi nhận kết quả mới được cập nhật. 4. Hệ thống xác định các bên liên quan (bác sĩ, bệnh nhân, PK ngoài…) 5. Hệ thống gửi thông báo đến từng bên qua kênh phù hợp (app, SMS, email…) 6. Các bên nhận được thông báo và có thể truy cập để xem chi tiết kết quả.
Alternative Path/ Flow	5a. Gửi thông báo qua ứng dụng nội bộ (app mobile hoặc portal) 5a1. Hệ thống xác định bệnh nhân hoặc bác sĩ có cài đặt ứng dụng nội bộ. 5a2. Hệ thống đẩy thông báo qua push notification hoặc popup trong app.
Exception Path/ Flow	2e. Kết quả nhận từ HT Lab bị lỗi hoặc thiếu dữ liệu 2e1. Hệ thống Lab trả kết quả nhưng dữ liệu không đầy đủ (thiếu mã xét nghiệm, định danh bệnh nhân...). 2e2. Hệ thống ghi nhận lỗi, không gửi thông báo. 2e3. Log lỗi được tạo và gửi cảnh báo đến quản trị viên hoặc kỹ thuật viên xét nghiệm. 2e4. Use case kết thúc 5e. Gửi thông báo thất bại do lỗi kết nối 5e1. Trong quá trình gửi thông báo (qua SMS/email/app), hệ thống gặp lỗi do mất kết nối với gateway hoặc server thứ ba. 5e2. Hệ thống retry sau 3 lần trong vòng 5 phút. 5e3. Nếu vẫn thất bại, hệ thống log lỗi và cảnh báo nội bộ.

	5e4. Use case kết thúc 6e. Actor không có quyền truy cập kết quả 6e1. Actor nhận được thông báo nhưng khi bấm vào xem kết quả, hệ thống kiểm tra và phát hiện actor không được phân quyền xem. 6e2. Hệ thống chặn truy cập và hiển thị thông báo “Bạn không có quyền xem kết quả này”. 6e3. Use case kết thúc
Business Rule	BR-01: Hệ thống chỉ gửi thông báo khi tất cả các xét nghiệm của một đợt chỉ định đã có kết quả. BR-02: Kết quả phải được kiểm duyệt và ký xác nhận bởi bác sĩ phụ trách trước khi thông báo được kích hoạt gửi tới người nhận. BR-03: Thông báo được gửi theo ưu tiên kênh liên lạc đã đăng ký: 1) App nội bộ, 2) SMS, 3) Email. BR-04: Thông báo phải chứa ID bệnh nhân ẩn danh, mã chỉ định và liên kết bảo mật (nếu có), không bao gồm kết quả chi tiết trong nội dung tin nhắn. BR-05: Trong trường hợp bệnh nhân thuộc phòng khám đối tác, hệ thống chuyển tiếp thông báo đến hệ thống bên ngoài qua API. BR-06: Nếu người nhận không có kênh liên lạc đã đăng ký (email/SĐT/app), thông báo không được gửi và hệ thống tạo log lỗi kèm cảnh báo quản trị. BR-07: Hệ thống không gửi lại thông báo nếu kết quả đã được gửi trước đó, trừ khi có thay đổi kết quả sau chỉnh sửa. BR-08: Log thông báo (bao gồm thời gian, kênh gửi, trạng thái gửi) phải được lưu tối thiểu 5 năm phục vụ kiểm toán y tế.
Non-Functional requirement	NFR-01 – Hiệu năng gửi: 95% thông báo phải được gửi đến người nhận trong vòng ≤ 10 giây kể từ thời điểm kích hoạt gửi. NFR-02 – Tính sẵn sàng: Dịch vụ thông báo có kết quả phải đạt tỷ lệ uptime ≥ 99.9%/tháng. NFR-03 – Đa kênh: Hệ thống phải hỗ trợ gửi thông báo qua tối thiểu 3 kênh: App mobile, SMS, Email, và sẵn sàng tích hợp thêm API phòng khám đối tác. NFR-04 – Bảo mật dữ liệu: Nội dung thông báo không được chứa thông tin nhạy cảm (kết quả, chẩn đoán…). Kết nối gửi phải dùng HTTPS, mã hóa TLS 1.2+.

	NFR-05 – Log & Audit Trail: Mọi thông báo gửi đi đều phải được ghi lại log bao gồm: người nhận, kênh, thời gian gửi, trạng thái gửi, mã chỉ định liên quan. NFR-06 – Khả năng mở rộng: Hệ thống phải xử lý tối thiểu 100.000 thông báo/ngày mà không ảnh hưởng hiệu năng. NFR-08 – Khả năng kiểm toán y tế: Giao diện hoặc API phải hỗ trợ truy xuất log thông báo theo mã bệnh nhân, mã chỉ định hoặc khoảng thời gian cụ thể.

UC 3: Phân quyền người dùng

Use Case ID	UC-SYS-003
Use Case Name	Phân quyền theo vai trò
Actor	Quản trị hệ thống (Admin)
Description	Admin gán các quyền cụ thể cho từng vai trò người dùng trong hệ thống (bác sĩ, lễ tân, bệnh nhân...).
Priority	Must have
Trigger	Admin chọn chức năng "Phân quyền theo vai trò" từ giao diện quản trị hệ thống.
Pre-Condition	Người dùng có quyền admin và đã đăng nhập hệ thống thành công.
Post-Condition	Các vai trò được gán quyền mới và cập nhật vào hệ thống; thay đổi có hiệu lực ngay lập tức.
Basic Path	1. Chọn chức năng “Phân quyền theo vai trò”. 2. Hệ thống hiển thị danh sách các vai trò hiện có (VD: Bác sĩ, Điều dưỡng, Lễ tân, Quản lý PK...). 3. Admin chọn 1 vai trò để cấu hình quyền. 4. Hệ thống hiển thị danh sách quyền tương ứng (VD: Tạo chỉ định, Xem kết quả, Cập nhật hồ sơ…). 5. Admin đánh dấu/ bỏ chọn các quyền phù hợp cho vai trò đó. 6. Xác nhận.

	7. Hệ thống cập nhật và hiển thị thông báo “Phân quyền thành công”.
Alternative Path	2a. Vai trò chưa tồn tại 2a1. Admin không tìm thấy vai trò cần phân quyền trong danh sách. 2a2. Admin nhấn “Tạo vai trò mới”. 2a3. Hệ thống hiển thị form tạo vai trò với các trường: Tên vai trò, Mô tả. 2a4. Admin nhập thông tin và nhấn “Lưu”. 2a5. Vai trò mới được lưu và quay lại bước 3. 2a6. Tiếp tục bước 4,5,6,7 4a. Gán quyền từ mẫu vai trò hệ thống 4a1.Admin chọn sử dụng mẫu có sẵn (ví dụ: Mẫu quyền cho bác sĩ, điều dưỡng…). 4a2. Hệ thống tự động gán danh sách quyền tương ứng với mẫu. 4a3. Admin có thể chỉnh sửa lại quyền nếu cần. 4a4. Tiếp tục bước 6,7
	1e. Người không có quyền truy cập 1e1. Người dùng không có quyền admin cố gắng truy cập chức năng phân quyền. 1e2. Hệ thống hiển thị cảnh báo: “Bạn không có quyền thực hiện thao tác này.” 1e3. Use case kết thúc 2e. Không tải được danh sách vai trò từ hệ thống 2e1. Hệ thống gặp lỗi kết nối cơ sở dữ liệu hoặc lỗi server khi truy xuất danh sách vai trò. 2e2. Giao diện không hiển thị được danh sách vai trò. 2e3. Use case kết thúc 6e. Lỗi ghi dữ liệu khi xác nhận phân quyền 6e1. Sau khi admin nhấn xác nhận, hệ thống không thể ghi dữ liệu xuống DB do lỗi hệ thống (ví dụ: timeout, disk full, lỗi mạng). 6e2. Hệ thống hiển thị lỗi kỹ thuật “Không thể lưu phân quyền”. 6e3. Use case kết thúc

Business Rule	BR‑01: Chỉ tài khoản Administrator (Admin) mới truy cập được chức năng "Phân quyền theo vai trò". BR‑02: Tên vai trò phải duy nhất trong toàn bộ hệ thống; không cho phép trùng. BR‑03: Mỗi vai trò phải có ≥ 1 quyền; hệ thống không lưu vai trò rỗng quyền. BR‑04: Danh mục quyền (permissions catalogue) là cố định và được quản lý ở cấp hệ thống; Use Case này chỉ gán hoặc bỏ gán quyền, không tạo/sửa/xóa quyền. BR‑05: Separation‑of‑Duties (SoD): nếu hai quyền được đánh dấu "xung đột", hệ thống không cho phép gán cả hai vào cùng một vai trò. BR‑06: Mọi thay đổi phân quyền có hiệu lực ngay lập tức; người dùng đã đăng nhập sẽ được áp dụng quyền mới ở lần yêu cầu (request) tiếp theo. BR‑07: Hệ thống ghi Audit Log đầy đủ (ai, khi nào, thay đổi quyền gì) và lưu trữ tối thiểu 5 năm. BR‑08: Các thay đổi phân quyền được bao bọc trong giao dịch ACID; nếu bất kỳ bước nào thất bại, toàn bộ thay đổi bị rollback.
Non-Functional Requirements	NFR‑01 – Hiệu năng: Thời gian tải danh sách vai trò và quyền ≤ 2 giây (p95) với 1.000 vai trò và 10.000 quyền. NFR‑02 – Khả dụng: Dịch vụ phân quyền phải đạt uptime 99.9 %/tháng. NFR‑03 – Bảo mật: Giao thức truyền dữ liệu dùng HTTPS/TLS 1.2+. - Kiểm tra CSRF & XSS cho form phân quyền. NFR‑04 – Đồng bộ phiên: Khi quyền của một vai trò thay đổi, cache phân quyền trên tất cả node ứng dụng được làm mới trong ≤ 30 giây. NFR‑05 – Khả năng mở rộng: Hệ thống hỗ trợ tối thiểu 10.000 vai trò & 1 triệu người dùng mà không giảm hiệu năng dưới ngưỡng NFR‑01. NFR‑06 – Khả năng kiểm toán: Audit log được mã hóa AES‑256, ghi dấu thời gian UTC, không thể sửa. Cung cấp API truy vấn cho bộ phận kiểm toán.

	NFR-07 – Tương thích thiết bị: Giao diện quản trị phải hiển thị tốt trên trình duyệt desktop Chrome, Edge, Firefox (hai bản phát hành gần nhất) với độ phân giải ≥ 1366×768. NFR-08 – Khôi phục sau thảm hoạ (DR): Sao lưu CSDL phân quyền mỗi 15 phút; mục tiêu khôi phục (RPO) ≤ 15 phút, thời gian khôi phục (RTO) ≤ 1 giờ.